Amendments to the Claims

The listing of claims will replace all prior versions, and listings of claims in the application.

1. *(Currently Amended)* A security method of controlling access of human beings to a secure item, the method comprising the steps of:

(1) retrieving an identification code from an identification object;

(1a) retrieving feature data from a memory using said identification code, said retrieved feature data representative of a plurality of facial features of a first person;

(2) capturing a plurality of facial features of a second person by taking pictures at different positions around said second person's head and generating feature data that is representative of facial features of said second person; and

(3) comparing said retrieved feature data of said first person to said second person feature data to determine security access for said second person, including

determining a plurality of errors that represent a difference between said plurality of facial features of said first person and a corresponding plurality of facial features of said second person,

determining an average error of said plurality of errors to determine security access of said second person.

2. *(Previously Presented)* The method of claim 1, further comprising the steps of:

(4) granting access to said second person if agreement between said retrieved feature data and said second person feature data is above a threshold; and

(5) denying access to said second person if agreement between said retrieved feature data and said second person feature data is below said threshold.

3. *(Previously Presented)* The method of claim 1, wherein step (1) comprises the step of reading a magnetic medium to retrieve said identification code.

4. *(Previously Presented)* The method of claim 1, wherein step (1) comprises the step of reading an optical medium to retrieve said identification code.

5. *(Previously Presented)* The method of claim 1, wherein step (1) comprises the step of reading a bar code to retrieve said identification code.

6. *(Previously Presented)* The method of claim 1, wherein step (1) comprises the step of reading a 2-dimensional bar code to retrieve said identification code.

7. *(Previously Presented)* The method of claim 1, wherein step (2) comprises the steps of:

(a) generating image data from said pictures;

(b) determining a first separation distance on a face of said second person using said image data;

(c) determining a second separation distance on said face of said second person using said image data; and

(d) normalizing said second separation distance relative to said first separation distance resulting in a ratio that is included in said second person feature data.

8. *(Previously Presented)* The method of claim 1,wherien step (2) comprises the steps of:

(a) generating image data from said pictures;

(b) determining an eye-to-eye separation on a face of said second person using said image data;

(c) determining a second separation distance on said face of said second person using said image data; and

(d) normalizing said second separation distance relative to said eye-to-eye separation resulting in a ratio that is included in said second person feature data.

9. *(Previously Presented)* The method of claim 1,wherein step (2) comprises the steps of:

(a) generating image data from said pictures;

(b) determining an eye-to-eye separation on a face of said second person using said image data;

(c) determining a forehead-to-chin separation on said face of said second person using said image data; and

(d) normalizing said forehead-to-chin separation relative to said eye-to-eye separation resulting in a ratio that is included in said feature data.

10. *(Currently Amended)* The method of claim 1,[[wherien]] wherein step (2) comprises the steps of:

(a) generating image data from said pictures;

(b) determining an eye-to-eye separation of said second person using said image data;

(c) determining an ear-to-ear separation of said second person using said image data; and

(d) normalizing said ear-to-ear separation relative to said eye-to-eye separation resulting in a ratio that is included in said second person feature data.

11. *(Previously Presented)* The method of claim 1, wherein step (2) comprises the steps of:

(a) generating image data from said pictures; and

(b) determining a separation distance between first and second features on a face of said second person, said second person feature data representative of said separation distance.

12. *(Previously Presented)* The method of claim 11, wherein step (b) comprises the steps of:

(i) locating a first eye and a second eye of said second person; and

(ii) determining an eye-to-eye separation between said first and second eye.

13. *(Previously Presented)* The method of claim 11, further comprising the steps of:

(c) determining a second separation distance between a third feature and a fourth feature on the face of said second person; and

(d) normalizing said second separation distance relative to said first separation distance.

14-15. *(Canceled)*.

16. *(Previously Presented)* The method of claim 1, further comprising the steps of:

(4) capturing said facial features of said first person; and

(5) storing said first person feature data in said memory prior to step (1).

17. *(Previously Presented)* The method of claim 1, wherein step (3) comprises the step of comparing a normalized forehead-to-chin separation of said first person with a normalized forehead-to-chin separation of said second person.

18. *(Previously Presented)* The method of claim 1, wherein step (3) comprises the step of comparing a normalized nostril-to-nostril separation of said first person with a normalized nostril-to-nostril separation of said second person.

19. *(Previously Presented)* The method of claim1, wherein step (3) comprises the step of comparing a normalized feature separation of said first person with a normalized feature separation of said second person.

20. *(Currently Amended)* A method of limiting security access to an authorized card owner, the method comprising the steps of:

(1) reading a medium of an access card to retrieve an identification code of the card owner;

(1a) retrieving feature data from a storage memory in a remote location using said identification code, said retrieved feature data representative of a plurality of facial features of the card owner;

(2) taking pictures of an applicant at different positions around said applicant's head and determining a plurality of facial features of the applicant using the pictures; and

(3) comparing said facial features of the card owner with said facial features of the applicant to determine access of the applicant, including

determining a plurality of errors that represent a difference between said plurality of facial features of the card owner and a corresponding plurality of facial features of the applicant,

determining an average error of said plurality of errors to determine security access of the applicant.

21. *(Previously Presented)* The method of claim 20, further comprising the steps of:

(4) granting access to the applicant if there is sufficient agreement between said applicant facial features and said card owner facial features; and

(5) denying access to the applicant if there is there is not sufficient agreement between said applicant facial features and said card owner facial features.

22. *(Currently Amended)* A method of determining if an applicant is the owner of an access card for security access purposes, the method comprising the steps of:

(1) reading a bar code on an access card, said bar code having feature data representative of a plurality of facial features of a card owner, said feature data including a normalized forehead-to-chin separation distance of said card owner;

(2) capturing a plurality of facial features of an applicant and generating applicant feature data that is representative of said applicant facial features, said step (2) comprising the steps of

(a) taking pictures of the applicant at different positions rotated around the applicant's head,

(b) determining an eye-to-eye separation of the applicant using said pictures, and

(c) determining a forehead-to-chin separation distance on a face of the applicant using said pictures, and normalizing said forehead-to-chin separation distance to said eye-to-eye separation;

(3) comparing said applicant feature data to said card feature data to determine security access, comprising

~~the step of~~ comparing said normalized forehead-to-chin separation distance of said applicant with said normalized forehead-to-chin separation distance of said card owner that is included in said card feature data

determining a plurality of errors that represent a difference between said plurality of facial features of the card owner and a corresponding plurality of facial features of the applicant,

determining an average error of said plurality of errors to determine security access of the applicant.

23-25. *(Canceled).*

26. *(Currently Amended)* A method of recording facial features of a person in a storage medium, the method comprising the steps of:

(1) taking pictures of the person at different positions with a camera that rotates around the person's head;

(2) generating feature data representative of facial features of the person, said feature data including a forehead-to-chin separation distance; and

(3) writing said feature data to said storage medium.

27. *(Original)* The method of claim 26, wherein step (3) comprises the step of writing said feature data to a magnetic medium on an access card.

28. *(Original)* The method of claim 26, wherein step (3) comprises the step of writing said feature data to an optical storage medium on an access card.

29. *(Original)* The method of claim 26, wherein step (3) comprises the step of writing said feature data to a bar code on an access card.

30. *(Original)* The method of claim 26, wherein step (3) comprises the steps of:

(a) writing an ID code associated with the person to an access card; and

(b) storing said feature data in a memory that is cataloged using said ID code.

31. *(Canceled).*

32. *(Previously Presented)* The method of claim 26, wherein step (2) of generating feature data comprises the steps of:

(a) determining an eye-to-eye separation distance using said picture;

(b) determining a forehead-to-chin separation distance using said pictures; and

(c) normalizing said forehead-to-chin separation distance relative to said eye-to-eye separation distance resulting in a ratio that is included in said feature data.

33-35. *(Canceled).*

36. *(Currently Amended)* A system for determining security access of an applicant, comprising:

a medium reader, for reading an access card medium to retrieve an identification code associated with a card owner;

a memory that stores facial feature data that is cataloged according to said identification code;

a rotating camera for taking pictures at different positions around said applicant's head [[,]] and generating feature data representative of facial features of said applicant; and

a processor for comparing said card feature data to said applicant feature data to determine security access, wherein said processor

determines a plurality of errors that represent differences between said stored facial feature data and said applicant feature data, and

determines an average error of said plurality of errors to determine security access of the applicant.

37. *(Previously Presented)* The system of claim 36, wherein said medium reader comprises a magnetic reader for reading a magnetic card medium on said access card to retrieve said identification code.

38. *(Previously Presented)* The system of claim 36, wherein said medium reader comprises a bar code reader for reading a bar code medium on said access card to retrieve said identification code.

39. *(Previously Presented)* The system of claim 38, wherein said bar code reader comprises a means for reading a 2 dimensional bar code.

40. *(Previously Presented)* The system of claim 36, further comprising:

a second processor for generating said applicant feature data based on image data that is representative of said picture, said processor determining a separation distance based on a first facial feature and a second facial feature, said applicant feature data including said separation distance.

41. *(Previously Presented)* The system of claim 39, further comprising a means for generating said image data from said pictures.

42. *(Previously Presented)* The system of claim 41, wherein said means for generating said image data comprises a computer scanner.

43. *(Previously Presented)* The system of claim 40, wherein said rotating camera is a digital camera, said digital camera generating said image data from said pictures.

44. *(Currently Amended)* A system for determining security access of an applicant, comprising:

a medium reader, for reading an access card medium to retrieve an identification code that identifies a card owner;

a memory that stores facial feature data that is cataloged according to said identification code;

a rotating camera for taking pictures at different positions around of the applicant's head, said rotating camera including a means for generating image data representative of said pictures; and

a processor coupled to said medium reader and said camera, said processor including computer program code for causing said processor to determine if the applicant is the card owner using said image data of said applicant and said card feature data, said computer program code comprising,

first program code means for causing said processor to determine [[an]] a plurality of applicant feature separations using said image data, said applicant feature separations representing a distance between a first feature and a second feature on a face of said applicant,

second program code means for causing said processor to access said memory using said identification code and to retrieve a plurality of card owner feature separations, said card owner feature separations representing a distance between a first feature and a second feature on a face of said card owner, and

third program code means for causing said processor to compare said card owner feature separations to said applicant feature separations and determine agreement for security access, wherein said third program means includes

program means for determining a plurality of errors that represent a difference between said plurality of card owner feature separations and a corresponding plurality of applicant feature separations, and

program means for determining an average error of said plurality of errors to determine security access.

45. *(Previously Presented)* The system of claim 44, wherein said program code means further comprises:

fourth program code means for causing said processor to grant access to the applicant if agreement is above a threshold; and

fifth program code means for causing said processor to deny access to the applicant if agreement is below a threshold.

46. *(Original)* The system of claim 44, wherein said medium reader is a bar code reader.

47. *(Currently Amended)* The system of claim 44, wherein said plurality of card owner feature separations are [[is]] normalized to an eye-to-eye separation of the card owner, and wherein said first program code means comprises program code means for causing said processor to determine an eye-to-eye separation of the applicant using the image data, and normalize said plurality of applicant feature separations relative to said eye-to-eye separation of the applicant.

48. *(Currently Amended)* The system of claim 44, wherein said plurality of card owner feature separations include [[is]] a normalized forehead-to-chin separation of the card owner, and wherein said plurality of applicant feature separations include [[is]] a normalized forehead-to-chin separation of the applicant.

49. *(Currently Amended)* The system of claim 44, wherein said plurality of card owner feature separations include [[is]] a normalized nostril-to-nostril separation of the card owner, and wherein said plurality of applicant feature separations [[is]] include a normalized nostril-to-nostril separation of the applicant.

50. *(Currently Amended)* The system of claim 46, wherein said plurality of card owner feature separations [[is]] include a normalized ear-to-ear separation of the card owner, and wherein said plurality of applicant feature separations include [[is]] a normalized ear-to-ear separation of the applicant.

51. *(Currently Amended)* An access card for use with a security system, said access card comprising a storage medium that stores an identification code associated with an owner of said access card, wherein said identification code catalogs feature data in a memory external to said access card, said feature data generated by ~~taking pictures at different positions~~ a camera that rotates around said owner's head and representative of facial features associated with said owner of the access card.

52. *(Previously Presented)* The access card of claim 51, wherein said medium is a bar code.

53. *(Original)* The access card of claim 51, wherein said feature data includes separation distances associated with said facial features of said card owner.

54. *(Previously Presented)* The system of claim 36, wherein said memory is in a remote location relative to at least one of said medium reader, said feature extractor, and said processor.

55. *(Previously Presented)* The method of claim 1, wherein the pictures are taken using a single rotating camera.

56. *(Previously Presented)* The method of claim 1, wherein the pictures are taken using multiple cameras that take pictures at multiple angles.

57. *(New)* The method of claim 1, wherein said first person is said second person.

58. *(New)* A method of controlling security access of humans, comprising:

retrieving an identification code from an identification object;

retrieving feature data from a memory using said identification code, said retrieved feature data representative of a plurality of facial features of a first person, said plurality of facial features normalized to an eye-to-separation of said first person;

capturing a plurality of facial features of a second person including taking pictures at different positions around said second person's head with a single camera that rotates around said second person's head, and generating applicant feature data from said pictures that is representative of facial features of said second person, including

locating a first eye and a second eye of said second person using said applicant feature data,

determining an eye-to-eye separation on a face of said second person using said applicant feature data,

determining a forehead-to-chin separation on said face of said second person using said applicant feature data,

normalizing said forehead-to-chin separation relative to said eye-to-eye separation resulting in a normalized forehead-to-chin ratio of said second person,

determining a nostril-to-nostril separation distance between a first nostril and a second nostril on said face of said second person using said applicant feature data,

normalizing said nostril-to-nostril separation distance relative to said eye-to-eye separation resulting in a normalized nostril-to-nostril separation ratio of said second person,

determining an ear-to-ear separation distance between a first ear and a second ear on said face of said second person using said applicant feature data,

normalizing said ear-to-ear separation distance relative to said eye-to-eye separation resulting in a normalized ear-to-ear ratio of said second person;

comparing said normalized ratios of said second person with corresponding ratios of said retrieved features data of said first person, including

determining a difference between a normalized nostril-to-nostril separation ratio of said first person and said normalized nostril-to-nostril separation ratio of said second person, resulting in a first ratio error,

determining a difference between a normalized forehead-to-chin separation ratio of said first person and said normalized forehead-to-chin separation ratio of said second person, resulting in a second ratio error,

determining a difference between a normalized ear-to-ear separation ratio of said first person and said normalized ear-to-ear separation ratio of said second person, resulting in a third ratio error, and

determining an average error of said first ratio error, said second ratio error, and said third ratio error to determine security access for said second person;

granting access to said second person if said average error is below a threshold; and

denying access to said second person if said average error is above said threshold.